

Stephen R. Sady
Chief Deputy Federal Public Defender
steve_sady@fd.org
Steven T. Wax
Federal Public Defender
steve_wax@fd.org
Ruben L. Iniguez
Assistant Federal Public Defender
ruben_iniguez@fd.org
101 S.W. Main Street, Suite 1700
Portland, Oregon 97204
503-326-2123 Telephone
503-326-5524 Facsimile
Attorneys for Defendant

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF OREGON
PORTLAND DIVISION

UNITED STATES OF AMERICA,

No. CR 10-475-KI

Plaintiff,

v.

MOHAMED OSMAN MOHAMUD,

Defendant.

**MEMORANDUM IN SUPPORT OF
MOTION TO DISCLOSE
FISA-RELATED MATERIAL
NECESSARY TO LITIGATE
MOTIONS FOR DISCOVERY AND
FOR SUPPRESSION OF THE FRUITS
OF FISA ACTIVITY**

TABLE OF CONTENTS

	PAGE
Table of Authorities.....	iii
Introduction.	1
A. The Defense Reasonably Believes FISA Was Invoked Based On The Government’s Notice And Non-FISA Discovery.....	1
B. FISA Authorizes Broad Surveillance And Search Of United States Citizens But Only If Certain Predicates Are Established..	2
C. Disclosure Of The FISA Warrants, Applications, And Fruits Should Be Made To Mr. Mohamud Under The FISA Provisions Calling For Disclosure Of Information To An Aggrieved Person When Necessary For Litigation Of Pretrial Motions Or When Required By Due Process..	5
1. Disclosure To The Defense Is Necessary To Make An Accurate Determination Of The Legality Of The Surveillance And Searches.	6
a. Defense Input Is Necessary To Address The Complex Questions Regarding Statutory Terms Such As “Foreign Power” And “Agent Of A Foreign Power” And Their Relationship To Criminal Activity..	7
b. The Issues Related To Mr. Mohamud’s Age Necessitate Disclosure To The Defense.	10
c. Significant Questions Exist Regarding Violation Of The Statutory Prohibition On Issuing Warrants Based On Activity That Is Protected By The First Amendment..	12
d. Defense Involvement Is Necessary To Address Questions Related To The Necessity For Use Of FISA.	13
e. Defense Involvement Is Necessary To Address Questions Related To Minimization Of The Government’s Intrusion.	14

f.	The Interplay Between The Motions To Suppress The FISA And Non-FISA Searches Is Complex And Requires Defense Participation For Full And Fair Litigation.	16
g.	The Length Of Surveillance And Searches In This Case Are Likely To Require Defense Involvement In The Litigation.	16
h.	Other Issues Common In Challenges To Searches And Wiretaps Are Likely To Be Present In This Case And Of Such Complexity That Defense Involvement Is Necessary For Fair Litigation.	17
2.	Independent Of The Need For Disclosure To Litigate Motions To Suppress, Due Process Requires That The Government Disclose The Bases For And Fruits Of Its FISA Searches And Surveillance.. . . .	18
D.	Whether Or Not The Court Orders Disclosure So That Mr. Mohamud Can Participate Meaningfully On His Motion To Suppress, This Court’s Review Of The FISA Warrant Or Warrants Is <i>De Novo</i>	23
E.	In The Event The Court Does Not Allow Defense Participation Regarding FISA Searches And Seizures, The Court’s Review Should Include Consideration Of Potential Constitutional Violations Stemming From The Statute And Its Application In This Case.	26
1.	The Standard And Procedures For Admissibility Of FISA-Generated Evidence, As Amended By The Patriot Act And Subsequently Interpreted By The Foreign Intelligence Surveillance Court Of Review – That Foreign Intelligence Gathering May Constitute Merely Some Purpose For The Electronic Surveillance Under FISA – Violates The Fourth Amendment’s Prohibition On Unreasonable Searches And Seizures.. . . .	27
a.	The Devolution Of The Standard For Issuing FISA Warrants.. . . .	28
(1)	The Initial Statutory Language of FISA.. . . .	28
(2)	Initial Court Interpretation: The “Primary Purpose” Standard.. . . .	28

(3)	The Patriot Act Amendments: The “Significant Purpose” Standard.	29
b.	The “Primary Purpose” Standard Was Essential To FISA’s Constitutionality.	32
(1)	The “Primary Purpose” Standard Predated FISA.	32
(2)	The Courts Adopted the Pre-Existing “Primary Purpose” Standard for FISA In Order to Preserve Its Constitutionality.	34
(3)	If the Warrants In This Case Were Issued Using The FISA Or FISCER Standard And Generated Information Supporting Investigation Of Criminal Activity, Any Extensions Violated The Fourth Amendment.	35
(4)	The “Significant Purpose” And/Or The FISCER’s More Diluted Standard Fail To Meet Fourth Amendment Requirements For Criminal Investigations.	36
(i)	FISA Authorizes Warrants In The Absence Of The Judicial Review Required Under The Fourth Amendment.	36
(ii)	FISA Orders Do Not Qualify As Warrants Under the Fourth Amendment.	38
(iii)	FISA Warrants Do Not Satisfy Traditional Probable Cause Standards.	39
(iv)	FISA Warrants Do Not Satisfy the Fourth Amendment’s Particularity Requirement.	40
(v)	The Fourth Amendment’s “Special Needs” Exception Does Not Apply To FISA.	42
2.	The <i>Ex Parte, In Camera</i> FISA Process Violates Due Process, A Defendant’s Rights To Be Present At All Critical Stages Of The Criminal Process, And His Right To The Effective Assistance Of Counsel.	44

3.	The FISA “Suppression” Process Unconstitutionally Interferes With The Article III Judicial Power.....	47
Conclusion	49

TABLE OF AUTHORITIES

	PAGE
<i>Alderman v. United States</i> , 394 U.S. 165 (1969).....	22, 46
<i>American Civil Liberties Union v. United States</i> , 538 U.S. 920 (2003).....	31
<i>Baker v. Carr</i> , 396 U.S. 186 (1962).....	48
<i>Berger v. New York</i> , 388 U.S. 41 (1967).....	40, 41
<i>Boumediene v. Bush</i> , 553 U.S. 723 (2008).....	47
<i>Brady v. Maryland</i> , 373 U.S. 83 (1963).....	15, 45
<i>Byars v. United States</i> , 273 U.S. 28 (1927).....	38
<i>Camreta v. Green</i> , 131 S. Ct. 2020 (2011).....	47
<i>Chimel v. California</i> , 395 U.S. 752 (1969).....	38
<i>City of Indianapolis v. Edmond</i> , 531 U.S. 32 (2000).....	43
<i>Cohens v. State of Virginia</i> , 19 U.S. (6 Wheat.) 264 (1821).....	47
<i>Coolidge v. New Hampshire</i> , 403 U.S. 443 (1971).....	24, 36
<i>Dalia v. United States</i> , 441 U.S. 238 (1979).....	38, 39

<i>Federal Radio Commission v. Nelson Brothers, Co.,</i> 289 U.S. 266 (1933).....	47
<i>Ferguson v. City of Charleston,</i> 532 U.S. 67 (2001).....	42, 43
<i>Franks v. Delaware,</i> 438 U.S. 154 (1978).....	17
<i>Hopt v. Utah,</i> 110 U.S. 574 (1884).....	45
<i>In re All Matters Submitted to the Foreign Intelligence Surveillance Court,</i> 218 F. Supp. 2d 611 (FISA Ct. 2002).	17
<i>In re Gault,</i> 387 U.S. 1 (1967).....	11
<i>In re Grand Jury Proceedings of Special April 2002 Grand Jury,</i> 347 F.3d 197 (7th Cir. 2003).	23
<i>In re United States of America's Application for a Search Warrant to Seize and Search Electronic Devices from Edward Cunnius,</i> No. 2:11-mj-00055-JPD-JLR, 2011 WL 991405 (W.D. Wash. Feb. 11, 2011).	15
<i>Johnson v. United States,</i> 333 U.S. 10 (1948).....	36
<i>Kendall v. United States,</i> 37 U.S. 524 (1838).....	48
<i>In re Kevork,</i> 634 F. Supp. 1002 (C.D. Cal. 1985).	37
<i>In re Kevork,</i> 788 F.2d 566 (9th Cir. 1986).	1
<i>LaChance v. Erickson,</i> 522 U.S. 262 (1998).....	44

<i>Marbury v. Madison</i> , 5 U.S. 137, 1 Cranch 137 (1803).....	21
<i>Maryland v. Pringle</i> , 540 U.S. 366 (2003).....	10
<i>Montejo v. Louisiana</i> , 129 S. Ct. 2079 (2009).....	44
<i>National Association for Advancement of Colored People v. Button</i> , 371 U.S. 415 (1963).....	12
<i>National Lawyers Guild v. Attorney General</i> , 96 F.R.D. 390 (S.D.N.Y. 1982).....	21
<i>In re Oliver</i> , 333 U.S. 257 (1948).....	45, 46
<i>Payton v. New York</i> , 445 U.S. 573 (1980).....	38
<i>Prince v. Massachusetts</i> , 321 U.S. 158 (1944).....	11
<i>United States v. Sarkissian</i> , 841 F.2d 959 (9th Cir. 1988).....	25, 34
<i>In re Sealed Case</i> , 310 F.3d 717 (FISA Ct. Rev. 2002).....	8, 14, 17, 28, 30 31, 37, 38, 43
<i>Skilling v. United States</i> , 130 S. Ct. 2896 (2010).....	26, 40
<i>Skinner v. Switzer</i> , 131 S. Ct. 1289 (2011).....	45
<i>Snyder v. Phelps</i> , 131 S. Ct. 1207 (2011).....	12
<i>Tennessee v. Lane</i> , 541 U.S. 509 (2004).....	44

<i>Texas v. Brown</i> , 460 U.S. 730 (1983).....	35
<i>Trustees of Philadelphia Baptist Association v. Hart's Ex'rs</i> , 17 U.S. 1 (1819).....	11
<i>Turner v. Rogers</i> , No. 10-10, 2011 WL 2437010 (U.S. June 20, 2011).....	44
<i>United States v. Abu-Jihaad</i> , 630 F.3d 102 (2d Cir. 2010).....	37
<i>United States v. Abuhamra</i> , 389 F.3d 309 (2d Cir. 2004).....	46
<i>United States v. Badia</i> , 827 F.2d 1458 (11th Cir. 1987).....	34
<i>United States v. Belfield</i> , 692 F.2d 141 (D.C. Cir. 1982).....	6, 16, 26, 46, 47
<i>United States v. Brown</i> , 484 F.2d 418 (5th Cir. 1973).....	33
<i>United States v. Burr</i> , 25 F. Cas. 30 (C.C.Va. 1807).....	20
<i>United States v. Butenko</i> , 494 F.2d 593 (3d Cir. 1974).....	33
<i>United States v. Campa</i> , 529 F.3d 980 (11th Cir. 2008).....	23
<i>United States v. Cardoen</i> , 898 F. Supp. 1563 (S.D. Fla. 1995).....	21
<i>United States v. Cavanagh</i> , 807 F.2d 787 (9th Cir. 1987).....	34, 41
<i>United States v. Comprehensive Drug Testing</i> , 621 F.3d 1162 (9th Cir. 2010).....	15

<i>United States v. Coplon</i> , 185 F.2d 629 (2d Cir. 1950).....	46
<i>United States v. Curtin</i> , 489 F.3d 935 (9th Cir.2007).	12
<i>United States v. Duggan</i> , 743 F.2d 59 (2d Cir. 1984).....	29, 34, 37
<i>United States v. Dumeisi</i> , 424 F.3d 566 (7th Cir. 2005).	19
<i>United States v. Fernandez</i> , 913 F.2d 148 (4th Cir. 1990).	20
<i>United States v. George</i> , 786 F. Supp. 11 (D.D.C. 1991).	21
<i>United States v. Gonzalez, Inc.</i> , 412 F.3d 1102 (9th Cir. 2005).	13
<i>United States v. Hammoud</i> , 381 F.3d 316 (4th Cir. 2004).	23
<i>United States v. Jacobson</i> , 466 U.S. 109 (1984).....	35
<i>United States v. Jayyousi</i> , No. 04-60001, 2007 WL 851278 (S.D. Fla. Mar. 15, 2007).	37
<i>United States v. Johnson</i> , 952 F.2d 565 (1st Cir. 1991).	34
<i>United States v. Kashmiri</i> , No. 09 CR 830-4, 2010 WL 4705159 (N.D. Ill. Nov. 10, 2010).....	8, 47
<i>United States v. Koyomejian</i> , 970 F.2d 536 (9th Cir. 1991).	41
<i>United States v. Leon</i> 468 U.S. 897, 926 (1984).....	25

<i>United States v. Libby</i> , 429 F. Supp. 2d 18 (D.D.C. 2006).....	23
<i>United States v. Libby</i> , 467 F. Supp. 2d 20 (D.D.C. 2006).....	20
<i>United States v. Lopez-Lima</i> , 738 F. Supp. 1404 (S.D. Fla. 1990).....	21
<i>United States v. Mejia</i> , 448 F.3d 436 (D.C. Cir. 2006).....	44
<i>United States v. Moussaoui</i> , 382 F.3d 453 (4th Cir. 2004).....	19
<i>United States v. Mubayyid</i> , 521 F. Supp. 2d 125 (D. Mass. 2007).	15, 23, 42, 45
<i>United States v. Nicholson</i> , 955 F. Supp. 588 (E.D. Va. 1997).....	26
<i>United States v. Nicholson</i> , No. 09-CR-40-BR, 2010 WL 1641167 (D. Or. April 21, 2010).	23
<i>United States v. Nixon</i> , 418 U.S. 683 (1974).....	21
<i>United States v. O'Hara</i> , 301 F.3d 563 (7th Cir. 2002).....	19
<i>United States v. Ott</i> , 827 F.2d 473 (9th Cir. 1987).....	6, 16
<i>United States v. Pelton</i> , 835 F.2d 1067 (4th Cir. 1987).....	34
<i>United States v. Poindexter</i> , 732 F. Supp. 142 (D.D.C. 1990).	21
<i>United States v. Posey</i> , 864 F.2d 1487 (9th Cir. 1989).....	27

<i>United States v. Prescott</i> , 581 F.2d 1343 (9th Cir. 1978).....	13
<i>United States v. Reynolds</i> , 345 U.S. 1 (1953).....	20, 21, 25
<i>United States v. Rosen</i> , 447 F. Supp. 538 (E.D. Va. 2006).....	8, 23, 24
<i>United States v. Salsedo</i> , 607 F.2d 318 (9th Cir. 1979).....	44
<i>United States v. Smith</i> , 321 F. Supp. 424 (C.D. Cal. 1971).....	27, 32
<i>United States v. Squillacote</i> , 221 F.3d 542 (4th Cir. 2000).....	23
<i>United States v. Thomson</i> , 752 F. Supp. 75 (W.D.N.Y. 1990).....	14, 15
<i>United States v. Truong Dinh Hung</i> , 629 F.2d 908 (4th Cir. 1980).....	27, 32, 33
<i>United States v. United States District Court for Easter Dist. of Michigan</i> , 407 U.S. 297 (1972).....	24, 27, 32
<i>United States v. Warsame</i> , 547 F. Supp. 2d 982 (D. Minn. 2008).....	8, 24
<i>United States v. Waters</i> , 627 F.3d 345 (9th Cir. 2010).....	12
<i>Vernonia Sch. District 47J v. Acton</i> , 515 U.S. 646 (1995).....	42

FEDERAL STATUTES

50 U.S.C. § 1801.....	5, 7, 8, 9, 10, 14
50 U.S.C. §§ 1802.....	23

50 U.S.C. §§ 1804.	2, 3, 4, 13, 28, 29, 36, 37
50 U.S.C. § 1805.	4, 7, 8, 17, 37, 39, 41, 48
50 U.S.C. §§ 1806.	6, 18
50 U.S.C. §§ 1821.	5
50 U.S.C. § 1824.	7
50 U.S.C. § 1825.	5, 6
50 U.S.C.A. 1801 <i>et. seq.</i>	1
18 U.S.C. § 2518(1).	13, 36, 41
Classified Information Procedures Act, 18 U.S.C. app. III.	18
Fed. R. Crim. P. 41.	36
H.R. Rep. 95-1283, Pt.1, 95th Cong., 2d Sess. 21 (1978).	8
PATRIOT ACT, Pub. L. No. 107-56, 115 Stat. 271 (2001).	29, 37
S. Rep. No. 95-701 (1978), <i>reprinted in</i> 1990 U.S.C.C.A.N. 4008.	14
S. Rep. No. 96-823 (1980), <i>reprinted in</i> 1980 U.S.C.C.A.N. 4294.	19, 20
S. Rep. No. 604, 95th Cong., 2d Sess. 9, <i>reprinted in</i> 1978 U.S.C.C.A.N. 3904.	1

MISCELLANEOUS

<i>Earl of Shaftsbury v. Shaftsbury</i> , 25 Eng. Rep. 121, 122-24 (1725).	11
---	----

Introduction

The Foreign Intelligence Surveillance Act (FISA) was enacted in 1978 in an effort to curb abuses regarding surveillance of United States citizens.¹ “The Act was intended to strike a sound balance between the need for such surveillance and the protection of civil liberties.” *In re Kevork*, 788 F.2d 566, 569 (9th Cir. 1986) (quoting S. Rep. No. 604, 95th Cong., 2d Sess. 9, *reprinted in* 1978 U.S.C.C.A.N. 3904, 3910). Although FISA includes important protections against unwarranted and overbroad government surveillance and searches, its use raises substantial risks that Americans will be subjected to unconstitutional invasions of their rights. This memorandum proceeds with five sections: 1) why the defense reasonably believes FISA was used in this case; 2) a description of the structure and requirements of the statute; 3) review of the potential issues in this case that make disclosure and suppression appropriate; 4) the importance of robust *de novo* review; and 5) preservation of challenges to the constitutionality of FISA generally and as applied in this case.

A. The Defense Reasonably Believes FISA Was Invoked Based On The Government’s Notice And Non-FISA Discovery.

On November 29, 2010, the government filed its FISA Notification advising that the government intended to “offer into evidence, or otherwise use or disclose . . . information obtained and derived from electronic surveillance and physical search” under FISA. CR 4. In addition, the government has made Classified Information Protection Act (CIPA) filings with the Court, which may also indicate that classified material generated by FISA activity is involved. CR 47, 49.

¹ In this pleading, unless otherwise noted, the most current version of FISA is relied upon. 50 U.S.C.A. 1801 *et seq.* (West 2011). As more information about this case becomes available, it may become necessary to reference previous versions of FISA.

Although the temporal scope of the government's use of FISA has not been disclosed, the complaint and discovery indicate early implementation of such activity.

The government's complaint makes several references to emails intercepted pursuant to "court authorized surveillance," which may indicate use of FISA warrants. CR 1 at 3-10. The discovery indicates that there was surveillance occurring during 2009, and a number of documents bear the information that the investigation was "derived from" investigation in March 2008. The sequence of events revealed in the discovery strongly suggests that the government's physical and electronic surveillance of Mr. Mohamud may have begun as early as 2008, and continued through his arrest on November 26, 2010.

B. FISA Authorizes Broad Surveillance And Search Of United States Citizens But Only If Certain Predicates Are Established.

FISA established a unique type of court – one that operates in secret and in which the government is the only entity permitted to appear. FISA authorizes issuance of two types of warrants by the Foreign Intelligence Surveillance Court (FISC) – those allowing electronic surveillance and those allowing physical searches. The statutory prerequisites are the same in most respects for both types of intrusions. Any application to the FISC must be made under oath by a federal officer and contain certain information and certifications. 50 U.S.C. §§ 1804 and 1823. In brief, an application for electronic surveillance must:

- provide the identity of the Federal officer making the application (§ 1804(a)(1));
- state the identity or description of the target (§ 1804(a)(2));
- include "a statement of the facts and circumstances relied upon by the applicant to justify his belief that . . . the target of the electronic surveillance

is a foreign power or an agent of a foreign power and each of the facilities or places at which the electronic surveillance is directed is being used, or is about to be used by a foreign power or an agent of a foreign power” (§ 1804(a)(3)(A) and (B));

- provide a “statement of proposed minimization procedures” (§ 1804(a)(4));
- provide a “description of the nature of the information sought and the type of communications or activities to be subjected to surveillance” (§ 1804(a)(5));
- set forth “certifications” by the Assistant to the President for National Security Affairs, an executive branch official or officials designated by the President from among those executive officers employed in the area of national security or defense and appointed by the President with the advice and consent of the Senate, stating as follows (§ 1804(a)(6)):
 - (A) the certifying official deems the information sought to be foreign intelligence information;
 - (B) a significant purpose of the surveillance is to obtain foreign intelligence information;
 - (C) such information cannot reasonably be obtained by normal investigative techniques,
 - (D) the type of foreign intelligence information being sought according to the categories describe in section 1801(e) of this title; and
 - (E) the basis for the certification that -
 - (i) the information sought is the type of foreign intelligence information designated; and
 - (ii) such information cannot reasonably be obtained by normal investigative techniques.

§ 1804(a)(6)(A)-(E). The statute also requires a summary statement of the means by which the surveillance will be effected and a statement whether physical entry is required to effect the surveillance, including:

- a statement of facts concerning all previous applications that have been made to any judge under this statute and action taken on each previous application;
- the specific period of time for which the electronic surveillance is required to be maintained.

Id. § 1804(a)(7) - (9). The Attorney General must personally review the application and determine that it satisfies the criteria and requirements set forth in the statute. § 1804(d).

Before the FISA court can approve electronic surveillance, it must make the following findings under § 1805(a):

- (1) the application was made by a Federal officer and approved by the Attorney General;
- (2) there is probable cause to believe that “the target of the electronic surveillance is a foreign power or an agent of a foreign power . . . and . . . each of the facilities or places at which the electronic surveillance is directed is being used or is about to be used by a foreign power or agent of a foreign power”;
- (3) the proposed minimization procedure meets the definition of minimization procedures under section 1804(h); and
- (4) the application contains all statements and certifications required.

FISA orders authorizing wiretaps are issued for certain specified periods of time, but can be extended pursuant to additional applications. § 1805(d)(1) and (2).

In accordance with § 1805(a)(4), if a target is a “United States person,” the FISC must find that the “certifications” under § 1804(a)(6)(E) – namely, that the information sought is (i) “the type of foreign intelligence information designated,” and (ii) “cannot reasonably be obtained by normal investigative techniques” – are “not clearly erroneous.” In contrast to foreigners, United States persons are provided protection for constitutionally protected activity: § 1805(a)(2)(A) provides

“[t]hat no United States person may be considered a foreign power solely upon the basis of activities protected by the first amendment.”

Critical to operation of FISA and review in this case are the definitions set out in 50 U.S.C. § 1801. “Foreign power” is defined in § 1801(a) to include foreign governments, groups they control, and groups engaged in terrorism. “Agent of a foreign power” is defined by a series of acts that distinguish between “any person who,” which includes a “United States person,” and “any person other than a United States person.” *Compare* 50 U.S.C. § 1801(b)(1) *and* (2). The types of acts that can support a warrant for a United States person are far more limited than those that can support a warrant for other people.

FISA authorizes any “aggrieved person” to move to suppress evidence obtained or derived from electronic surveillance on the grounds that “the information was unlawfully acquired” or “the surveillance was not made in conformity with an order of authorization or approval.” § 1806(e)(1) and (2). FISA defines the phrase “aggrieved person” as “a person who is the target of an electronic surveillance or any other person whose communications or activities were subject to electronic surveillance.” § 1801(k).

The prerequisites for a search and authorization to seek suppression of the fruits of any such search are found in 50 U.S.C. §§ 1821-25. They are similar to those for electronic surveillance.

C. Disclosure Of The FISA Warrants, Applications, And Fruits Should Be Made To Mr. Mohamud Under The FISA Provisions Calling For Disclosure Of Information To An Aggrieved Person When Necessary For Litigation Of Pretrial Motions Or When Required By Due Process.

While much litigation over classified material takes place *ex parte*, Congress, in FISA, recognized the potential necessity for defense access to classified material and participation by an

aggrieved party in litigation over the legality of FISA-derived surveillance and searches. Congress and the courts have also recognized that access by the defense to classified material may also be required by the Due Process Clause of the Constitution.

1. Disclosure To The Defense Is Necessary To Make An Accurate Determination Of The Legality Of The Surveillance And Searches.

FISA specifically includes a provision for suppression of unlawfully obtained evidence: When a court determines that electronic surveillance or a physical search “was not lawfully authorized or conducted, it shall . . . suppress the evidence which was unlawfully obtained or derived from the electronic surveillance or physical search of the aggrieved person.” 50 U.S.C. §§ 1806(g) (electronic surveillance), 1825(h) (physical search). In determining the legality of surveillance, “the court may disclose to the aggrieved person, under appropriate security procedures and protective orders, portions of the application, order, or other materials relating to the surveillance only where such disclosure is necessary to make an accurate determination of the legality of the surveillance.” 50 U.S.C. §§ 1806(f) (electronic surveillance), § 1825(g) (physical searches). Disclosure is, therefore, warranted when a court needs a defense attorney’s input to decide whether to suppress evidence obtained through a FISA order.

While courts have not allowed defense participation in suppression hearings, the decisions have articulated several principles that support defense participation on Mr. Mohamud’s behalf. In *United States v. Belfield*, 692 F.2d 141, 147 (D.C. Cir. 1982), the court noted that the issues were not “complex,” suggesting that if they were, disclosure would be required. In *United States v. Ott*, 827 F.2d 473, 476 (9th Cir. 1987), the court identified issues such as misrepresentations of fact,

vague identification, or records showing overbroad surveillance. Here, many potential bases for suppression based on unlawful surveillance are present, and the issues are complicated.

- a. Defense Input Is Necessary To Address The Complex Questions Regarding Statutory Terms Such As “Foreign Power” And “Agent Of A Foreign Power” And Their Relationship To Criminal Activity.*

FISA involves the unique substantive requirement for probable cause of proof that a person is a foreign power or an agent of a foreign power. Instead of directing a judge to find probable cause to believe that the fruits or evidence of a crime may be found, a FISC judge must find that there is probable cause to believe that the target is a foreign power or agent of a foreign power and that the facilities or locations sought to be searched are being used, or are about to be used, by a foreign power or agent of a foreign power. 50 U.S.C. § 1805(a)(2). The same probable cause finding is required for physical searches, except that the judge must find that “the premises or property to be searched is or is about to be owned, used, possessed by, or is in transit to or from a foreign power or an agent of a foreign power.” 50 U.S.C. § 1824(a)(2)(B). What type of proof can satisfy the substantive probable cause requirement is set out in the definitional sections of 50 U.S.C. § 1801.

The probable cause issues are complex in this case. Under the statutory definitions, no warrant should have issued under the “foreign power” (50 U.S.C. § 1801(a)) section of the statute because Mr. Mohamud does not meet those criteria. Nor, by definition, can he be an agent of a foreign power under § 1801(b)(1) because that section only applies to “any person *other than a United States person.*” 50 U.S.C. § 1801(b)(1) (emphasis added). Thus, any warrant should have issued under 50 U.S.C. § 1801(b)(2). Precisely what must be found is not, however, clear.

One portion of the statute focuses on a target's status "as a foreign power" or as an "agent of a foreign power," rather than on involvement in criminal activity. 50 U.S.C. §§ 1805(a)(2)(A), 1805(a)(3), 1824(a)(2)(A). Some courts that have written on the standard have focused there. *See, e.g., United States v. Warsame*, 547 F. Supp. 2d 982, 991 (D. Minn. 2008). Others have held that no probable cause of past or present criminal activity need be shown. *United States v. Kashmiri*, No. 09 CR 830-4, 2010 WL 4705159, at *3 (N.D. Ill. Nov. 10, 2010). That is, however, an overly limited view of the statutory requirements. With respect to a United States person, there must be a showing of criminal activity.

It is explicit in the definitional section that FISA requires proof that a person's activities are or may be in violation of the criminal laws of the United States. 50 U.S.C. §§ 1801(b)(2)(A) and (B), (c)(1), (d). The need to establish a relationship to criminal activity for United States persons is made clear in the legislative history of FISA. H.R. Rep. 95-1283, Pt.1 at 36, 95th Cong., 2d Sess. 21 (1978). The only decision ever issued by the Foreign Intelligence Surveillance Court of Review (FISCR) made the same point. *In re Sealed Case*, 310 F.3d 717, 738 (FISA Ct. Rev. 2002). The definition of agent of a foreign power for United States persons "is closely tied to criminal activity." *In re Sealed Case*, 310 F.3d at 723.

The definitions are, however, confusing. Subsection 1801(b)(2)(A) allows a warrant on a showing that a person is acting in a manner that "may involve" a violation of a statute. Subsection (2)(B) requires that the activities "involve or are about to involve" violation of a statute. This is a higher standard. Subsection (b)(2)(C), through the definition in subsection (c)(1) requires acts that "are" a violation of the criminal laws. This is a higher standard. *See United States v. Rosen*, 447 F.

Supp. 2d 538, 549 (E.D. Va. 2006) (discussing lesser showing under § 1801(b)(2)(A)). The fact that some courts appear to write the relation to criminal activity out of the calculus underscores the confusion in the courts and perhaps in government briefing. Full disclosure and defense involvement in addressing these different and complex standards is necessary.

The teenaged Mr. Mohamud does not appear to meet the definitions of a “foreign power.” With respect to “agent of a foreign power,” FISA’s distinction between United States persons and non-United States persons provides a far more limited authority to conduct surveillance and searches of United States persons. For example, warrants may be issued if there is sufficient justification to believe a foreigner “engages in international terrorism or activities in preparation therefore.” 50 U.S.C. § 1801(b)(1)(C).² Such a showing will not, however, justify a FISA warrant against a United States person. Instead, any such acts must be done “knowingly” “for or on behalf of a foreign power.” 50 U.S.C. § 1801(b)(2)(C).

Most of the authority for a warrant against a United States person can be readily determined to be inapplicable in this case. There is no hint that Mr. Mohamud was engaging in clandestine

² Section 1801(c) defines “international terrorism” as follows:

(c) “International terrorism” means activities that -

- (1) involve violent acts or acts dangerous to human life that are a violation of the criminal laws of the United States or of any State, or that would be a criminal violation if committed within the jurisdiction of the United States or any State;
- (2) appear to be intended -
 - (A) to intimidate or coerce a civilian population;
 - (B) to influence the policy of a government by intimidation or coercion; or
 - (C) to affect the conduct of a government by assassination or kidnaping; and
- (3) occur totally outside the United States, or transcend national boundaries in terms of the means by which they are accomplished, the persons they appear intended to coerce or intimidate, or the locale in which their perpetrators operate or seek asylum.

intelligence gathering (§ 1801(b)(2)(A)), acting under the direction of an intelligence network of a foreign power (§ 1801(b)(2)(B)), or that he entered the United States under a false or fraudulent identity (§ 1801(b)(2)(D)). The only possible bases on which a warrant could have been sought and issued would then appear to be 50 U.S.C. § 1801(b)(2)(C) and (E). No information appears to support a claim that Mr. Mohamud was “knowingly” engaged in “sabotage or international terrorism on behalf of a foreign power.” Defense involvement in examination of the facts presented to the FISC is necessary to ensure that FISA was not improperly utilized.

Because FISA requires proof of criminal activity to support surveillance or search of a United States person, significant questions may also arise involving the interplay between the FISA standard and the long-standing rules that probable cause requires “a reasonable ground for belief of guilt,” and “the belief of guilt must be particularized with respect to the person to be searched or seized.” *See Maryland v. Pringle*, 540 U.S. 366, 371 (2003). The defense has not received evidence that Mr. Mohamud was engaged in criminal activity prior to the communications from government agents. Defense involvement will therefore be necessary to counter arguments the government is likely to make in support of its warrants.

b. The Issues Related To Mr. Mohamud’s Age Necessitate Disclosure To The Defense.

To the extent FISA activity pre-dated August 11, 2009,³ this Court will be considering novel legal questions. Juveniles stand in a unique legal posture. As a general proposition, governmental entities are charged with significant responsibilities to protect and to care for juveniles.

³ Mr. Mohamud turned 18 years old on August 11, 2009.

The common law doctrine of *parens patriae* involves the power and duty of the state to act as sovereign and guardian over juveniles outside the protection of their parents. BLACK'S LAW DICTIONARY 1114 (6th ed. 1990); *Earl of Shaftsbury v. Shaftsbury*, 25 Eng. Rep. 121, 122-24 (1725); *Prince v. Massachusetts*, 321 U.S. 158, 166 (1944) (recognizing the state as *parens patriae* when restricting the parent's control by requiring school attendance and regulating child labor). See *In re Gault*, 387 U.S. 1, 17 (1967). The rights and obligations under the *parens patriae* doctrine passed from the King to the federal and state governments after the Revolution, as first argued in *Trustees of Philadelphia Baptist Ass'n v. Hart's Ex'rs*, 17 U.S. 1, 13 (1819).

The special care a government must take in regards to juveniles, within the criminal justice system, is reflected in the significant authority against using juveniles as informants. Andrea L. Dennis, *Collateral Damage? Juvenile Snitches in America's "Wars" on Drugs, Crime, and Gangs*, 46 AM. CRIM. L. REV. 1145, 1175-1189 (2009). This reluctance exists, in part, because governments should not place juveniles in harm's way. Charoletta J. Ranson, *Does the End Justify the Means? Use of Juveniles As Government Informants, Helpful to Society While Harmful To The Child*, 20 J. Juv. L. 108, 125 (1999) ("The best interest of the child should be at the forefront of any decision to use a juvenile as an undercover informant. The use of children as such should not be permissible when the crime committed by the child is divertable."). "The child's safety outweighs the potential benefit to society. The end does not justify the means." *Id.* at 126. The same reasoning should apply to FISA surveillance, especially given the obstacles to legal agency by minors.

If the government went to the FISC or otherwise conducted surveillance while Mr. Mohamud was a juvenile, questions related to his age will be relevant to defense input on the reasonableness

of the government's actions under FISA and the Fourth Amendment. These complex issues warrant disclosure and full defense involvement.

c. Significant Questions Exist Regarding Violation Of The Statutory Prohibition On Issuing Warrants Based On Activity That Is Protected By The First Amendment.

The prohibition in FISA against issuance of a warrant based solely upon First Amendment activities may be relevant in this case. The discovery includes material written and read by Mr. Mohamud that pre-date government contacts. The material available to the defense is all protected by the First Amendment. In fact, the timing of the arrest appears to be based on the government's theory that, until that moment, no crime had been committed.

Various means of expression, including the use of books and writings, both in hard copy and on the internet, and the expressed desire to study at a foreign university, raise challenging issues regarding the rights to be exposed to and express ideas and beliefs that may be at odds with or even repugnant to the general public. *See Snyder v. Phelps*, 131 S. Ct. 1207 (2011) (First Amendment protects picketers at military funeral); *see also United States v. Waters*, 627 F.3d 345, 354-55 (9th Cir. 2010); *United States v. Curtin*, 489 F.3d 935, 956 (9th Cir. 2007) (en banc). Activities such as expressing support, urging others to express support, gathering information, distributing information, writing about exercise while in jail, raising money for political causes, or donating money for political causes, are all protected and cannot serve as a basis for probable cause. *See Nat'l Ass'n for Advancement of Colored People v. Button*, 371 U.S. 415, 444-45 (1963) (The "First Amendment protects expression and association without regard to the race, creed, or political or religious affiliation of the members of the group which invokes its shield, or to the truth, popularity, or social

utility of the ideas and beliefs which are offered.”). Exercise of constitutional rights cannot be used as a component of probable cause. *Cf. United States v. Prescott*, 581 F.2d 1343, 1351-52 (9th Cir. 1978) (refusal of consent did not justify search).

This case likely involves issues that will require a careful adversary process to ensure enforcement of FISA’s First Amendment protections. First Amendment issues are often complex, with interests at stake that extend beyond the parties engaged in the litigation. As a result, it is necessary for disclosure to the defense to assist the Court in addressing these issues.

d. Defense Involvement Is Necessary To Address Questions Related To The Necessity For Use Of FISA.

In order to limit intrusions under FISA, Congress allowed its use only when the Attorney General certifies “that such information cannot reasonably be obtained by normal investigative procedures.” 50 U.S.C. § 1804(a)(6)(C); 1823(a)(6)(C). This provision is similar to that found in 18 U.S.C. § 2518(1)(c) (warrant application must include “full and complete statement as to whether or not other investigative procedures have been tried and failed or why they reasonably appear to be unlikely to succeed if tried or to be too dangerous).” There is scant guidance on the necessity issue under FISA. It is often complex under Title III. *See, e.g., United States v. Gonzalez, Inc.*, 412 F.3d 1102, 1111-15 (9th Cir. 2005). The information available to Mr. Mohamud suggests that significant issues exist with respect to the bases for the government’s belief that use of FISA was necessary. Disclosure and defense involvement on this important issue is necessary.

e. Defense Involvement Is Necessary To Address Questions Related To Minimization Of The Government's Intrusion.

Under FISA, as under the Title III wiretap statute, the government is required to demonstrate it has minimized its intrusions. *See* 50 U.S.C. §§ 1801(h); 1802 (a)(1)(C); 1804(a)(4); 1805(a)(3); 1806(a); 1821(4); 1822(a)(1)(A)(iii); 1823(a)(4); 1824(a)(3), and (c)(2)(A); 1825(a); 1861(g); 1881a(e) and (g)(2)(A)(ii) and (i)(2)(C); 1881b(b)(D) and (c)(1)(C) and (c)(3)(C) and (d)(2); 1881c(b)(4) and (c)(1)(C) and (c)(3)(C) and (d)(2).

[The] minimization procedures are designed to protect, as far as reasonable, against the acquisition, retention, and dissemination of nonpublic information which is not foreign intelligence information. If the data is not foreign intelligence information as defined by the statute, the procedures are to ensure that the government does not use the information to identify the target or third party, unless such identification is necessary to properly understand or assess the foreign intelligence information that is collected.

In re Sealed Case, 310 F.3d at 731 (citing § 1801(h)(2)).

The statute requires three specific types of minimization to protect distinct interests. 50 U.S.C. § 1801. First, by minimizing acquisition, Congress envisioned that surveillance should be discontinued where the target is not a party to the communications. Second, by minimizing retention, Congress intended that information acquired, which is not necessary for obtaining, producing, or disseminating foreign intelligence information, be destroyed where feasible. Third, by minimizing dissemination, Congress intended that even lawfully retained information should only be divulged to those officials with a specific need. *In re Sealed Case*, 310 F.3d at 731. “The FISA minimization procedures were enacted ‘generally to parallel the minimization provision in existing [electronic surveillance] law.’” *United States v. Thomson*, 752 F. Supp. 75, 80 (W.D.N.Y. 1990) (quoting S. Rep. No. 95-701, at 39 (1978), *reprinted in* 1990 U.S.C.C.A.N. 4008). “[A]bsent a

charge that the minimization procedures have been disregarded completely, the test of compliance is whether a good faith effort to minimize was attempted.” *Thomson*, 752 F. Supp. at 80 (citations omitted); see *United States v. Mubayyid*, 521 F. Supp. 2d 125, 134 (D. Mass. 2007) (noting that the “Court must take into account the complex and time-intensive nature of piecing together, and making sense of, the myriad pieces of information gathered during a lengthy surveillance”).

The need to ensure proper constraints in searching computers was underscored in *United States v. Comprehensive Drug Testing (CDT)*, 621 F.3d 1162 (9th Cir. 2010) (en banc). *CDT* was relied upon in *In re United States of America’s Application for a Search Warrant to Seize and Search Electronic Devices from Edward Cunniss*, No. 2:11-mj-00055-JPD-JLR, 2011 WL 991405, at *14 (W.D. Wash. Feb. 11, 2011). There, upon denying a warrant application, the magistrate judge found that the government should not be given the “authority to scour all data contained in the seized digital devices” nor the “authority to obtain a second warrant” based on data found outside the scope of the first warrant, whether in plain view or not. It appears that complex computer search issues will be present in this case.

The potential minimization problem here is demonstrated by the apparent breadth of the surveillance. The amount of traffic the government indicates it seized and has provided that it asserts is neither covered by Rule 16 nor *Brady v. Maryland*, 373 U.S. 83 (1963) (CR 28 at 14) shows that minimization is at least an issue. The broad communications with family and friends that were listened in on, while assisting the defense to the extent they are innocuous, show that reasonable limits were not placed on the surveillance. Based on defense investigation and review of discovery to date, this case involves indications that “the question of legality” of the surveillance and seizures

may be complicated by factors such as indications of “surveillance records which include a significant amount of non-foreign intelligence information, calling into question compliance with the minimization standards contained in the order.” *Belfield*, 692 F.2d at 147(internal quotation and footnote omitted); *see also Ott*, 827 F.2d at 476.

f. The Interplay Between The Motions To Suppress The FISA And Non-FISA Searches Is Complex And Requires Defense Participation For Full And Fair Litigation.

On November 2, 2009, Mr. Mohamud was contacted by local law enforcement authorities based on allegations of purely local conduct. The allegations turned out to be unfounded. It appears that surveillance prior to November 1, 2009, led in part to the searches during the local criminal investigation. As described in the motion to suppress non-FISA activity, the state officers brought in federal authorities despite the purely local nature of their investigation. This led to searches and seizures far beyond the reasonable scope of any consent given for investigation of the state activity. Disclosure of FISA material is necessary for the defense to evaluate causation regarding state actions, as well as to obtain information regarding issues of use and taint for any post-search surveillance.

g. The Length Of Surveillance And Searches In This Case Are Likely To Require Defense Involvement In The Litigation.

It will likely be necessary to carefully examine the dates, in sequence, of all FISA orders in this case to determine on what bases extensions were granted, whether the requests included the requisite showing of necessity, and whether there were any lapses of time during which wiretapping continued. The statutory scheme contemplates a seamless web: when a FISA order expires, if the government wishes to continue the intrusion, the expiring order must be replaced by an extension order, which, in turn, may be obtained only on the basis of a proper FISA application.

§§ 1805(d)(1)-(3); 1824(d)(1)-(3). An extension application may be bolstered or undermined by what has already been obtained. Moreover, a wiretap or search that continues to run past the expiration date of the FISA order that originally authorized it is just as unauthorized as a wiretap that is initiated without any FISA order at all. Finally, the existence of any pre-FISA surveillance must be determined in order to litigate any FISA procedures as fruits of potential warrantless intrusions. Full adversarial consideration of these issues after disclosure of all applications and warrants is necessary.

h. Other Issues Common In Challenges To Searches And Wiretaps Are Likely To Be Present In This Case And Of Such Complexity That Defense Involvement Is Necessary For Fair Litigation.

The FISA applications may contain intentional or reckless material falsehoods or omissions, and the surveillance therefore may violate the principles of *Franks v. Delaware*, 438 U.S. 154 (1978). In other cases, the government has confessed error relating to “misstatements and omissions of material facts” that it had made in its FISA applications. *In re All Matters Submitted to the Foreign Intelligence Surveillance Court*, 218 F. Supp. 2d 611, 620-21 (FISA Ct. 2002), *abrogated on other grounds, In re Sealed Case, supra*. Disclosure is, therefore, necessary so that, based on defense analysis, this Court can conduct a *Franks* hearing at which Mr. Mohamud will have the opportunity to inquire into whether the affiants before the FISA court intentionally or recklessly made materially false statements or omitted material information from the FISA applications. In this regard, significant questions are likely to exist regarding the extent to which Mr. Mohamud was portrayed as an agent of a foreign power, whether the primary purpose of the electronic surveillance was to obtain evidence of domestic criminal activity or foreign intelligence information, whether the

government made the required certifications in the FISA application, and whether it properly obtained extensions of FISA orders.

In addition, there is at least some history of using warrantless surveillance as the basis for FISA requests. *See* James Bamford, *THE SHADOW FACTORY*, (Doubleday 2008) at 117 (“By the time the [National Security Agency] operation was up and running in the fall of 2001, between 10 and 20 percent of all the requests coming to the FISA court were tainted by what is known in the legal profession as ‘the fruit of the poisonous tree,’ that is, the warrantless program.”). Inquiry should be made into this issue as well.

In order to litigate these complex FISA and non-FISA issues, full disclosure to and involvement by the defense is necessary and appropriate.

2. Independent Of The Need For Disclosure To Litigate Motions To Suppress, Due Process Requires That The Government Disclose The Bases For And Fruits Of Its FISA Searches And Surveillance.

In addition to, and independent of, the need to disclose the FISA warrants, affidavits, and fruits in order for the Court to effectively consider Mr. Mohamud’s motion to suppress, the Court should order disclosure as a matter of due process. FISA specifically requires disclosure under the Due Process Clause, directing courts to deny a defendant’s motion under FISA “except to the extent that due process requires discovery or disclosure.” 50 U.S.C. §§ 1806(g); 1825(h); 1845(g)(2). These provisions of FISA are consistent with the procedures set out in the Classified Information Procedures Act, 18 U.S.C. app. III (CIPA), and with the general body of law on discovery.

CIPA sets out procedures for the disclosure and use of classified information in criminal cases. 18 U.S.C. app. III at §§ 4, 6. In sum, when classified information is material to the defense,

the government is given four options. First, it can disclose the material to security-cleared counsel. Second, it can declassify the material and disclose it. Third, it can, in some circumstances, provide an unclassified summary. Fourth, if it refuses any of the three options for disclosure, it faces exclusion of evidence or dismissal of its case. 18 U.S.C. app. III at § 6(c) and (e).

The mechanisms and procedures for disclosure are set out in § 4 of CIPA. CIPA is intended to ensure that a defendant in a criminal trial obtains the information he needs to present his defense consistent with national security needs. Indeed, the “fundamental purpose” of CIPA “is to protect [] and [] restrict the discovery of classified information in a way that does not impair the defendant’s right to a fair trial.” *United States v. Dumeisi*, 424 F.3d 566, 578 (7th Cir. 2005) (quoting *United States v. O’Hara*, 301 F.3d 563, 569 (7th Cir. 2002)). In debating the statute, Congress confirmed that CIPA “rests on the presumption that the defendant should not stand in a worse position, because of the fact that classified information is involved, than he would without [CIPA].” S. REP. NO. 96-823, at 9 (1980), *reprinted in* 1980 U.S.C.C.A.N. 4294, 4302.

These principles have been adhered to in the one trial this country has experienced deriving from the attacks of September 11, 2001. In *United States v. Moussaoui*, 382 F.3d 453, 477 (4th Cir. 2004), the court stated that CIPA “adequately conveys the fundamental purpose of a substitution; to place the defendant, as nearly as possible, in the position he would be in if the classified information . . . were available to him.” As stated in another high-profile case involving potential harm to an outed CIA agent, when addressing a discovery request pursuant to CIPA:

[T]he Court should not take into account or balance the government’s national security interest in protecting the classified information from disclosure. Rather, the statute makes clear that the Court’s only inquiry is whether the proposed substitutions provide the defendant substantially the same ability to present his defense.

United States v. Libby, 467 F. Supp. 2d 20, 25 (D.D.C. 2006) (citing 18 U.S.C. app. III, § 6(c)); *see also United States v. Fernandez*, 913 F.2d 148, 162 (4th Cir. 1990). As reflected in the Senate Report on CIPA, the Act was designed so the government could decide whether to go forward with a case by making a pretrial assessment of the “potential damage to national security” that may result. S. REP. NO. 96-823, at 1 (1980), *reprinted in* 1980 U.S.C.C.A.N. 4294, 4294.

The question of what information due process requires to be disclosed is the same when considering FISA-derived, and other classified, evidence, as it is for all exculpatory evidence in a criminal case. This basic principle has its origins in *United States v. Burr*, 25 F. Cas. 30 (C.C.Va. 1807), where the Court concluded that a criminal defendant may issue a subpoena to the President of the United States to compel his attendance as a witness if helpful to the defense. The Court also noted that “there may be matter, the production of which the court would not require” to be disclosed if it is immaterial to the defense and the Executive asserts that its disclosure would be imprudent. *Burr*, 25 F. Cas. at 37. However, Chief Justice Marshall went on to state that, if the information was in fact material to the defense, denial of the accused’s request for that information in favor of the Executive’s privilege would be an undesirable course of action. *Burr*, 25 F. Cas. at 37.

The Supreme Court provided additional guidance regarding state secrets in criminal trials in *United States v. Reynolds*, 345 U.S. 1 (1953). *Reynolds* noted that “[i]n each case, the showing of necessity which is made [by the party seeking disclosure] will determine how far the court should probe in satisfying itself that the occasion for invoking the privilege is appropriate.” *Id.* at 11.

[T]he Government can invoke its evidentiary privileges only at the price of letting the defendant go free. The rationale of the criminal cases is that, since the Government which prosecutes an accused also has the duty to see that justice is done, it is

unconscionable to allow it to undertake prosecution and then invoke its governmental privileges to deprive the accused of anything which might be material to his defense.

345 U.S. at 12 (citing *United States v. Andolschek*, 142 F.2d 503 (2d Cir. 1944); *United States v. Beekman*, 155 F.2d 580 (2d Cir. 1946)). “The Supreme Court has authoritatively decided that in conflict between the fair trial rights of a defendant in a criminal case and the general prerogatives of the President, the former prevails.” *United States v. Poindexter*, 732 F. Supp. 142, 162 (D.D.C. 1990) (citing *United States v. Nixon*, 418 U.S. 683 (1974); *Marbury v. Madison*, 5 U.S. 137, 1 Cranch 137 (1803)).

The fact that information “is classified should not be considered when determining its admissibility.” *United States v. Cardoen*, 898 F. Supp. 1563, 1571 (S.D. Fla. 1995) (quoting *United States v. Lopez-Lima*, 738 F. Supp. 1404, 1407 (S.D. Fla. 1990)). Because the defendant’s constitutional right to a fair trial is at stake, the analysis of materiality is not a rigorous one. The necessary inquiry pre-trial with respect to classified as well as unclassified documents is whether there is an indication that the evidence would play an important role in uncovering admissible evidence, aiding witness preparation, corroborating testimony, or assisting impeachment or rebuttal. *United States v. George*, 786 F. Supp. 11, 13 (D.D.C. 1991) (analyzing defendant’s claim of materiality of classified information under Fed. R. Crim. P. 16(a)(1)(C)); *National Lawyers Guild v. Attorney General*, 96 F.R.D. 390, 398 n.18 (S.D.N.Y. 1982) (noting that “[i]n the criminal context, the court must consider the defendant’s need for information that is material to the preparation of his defense”). Where the defendant expects to elicit sensitive national security information from the Executive, the proper remedy is to ensure CIPA compliance rather than to preclude discovery and examination of the materials. *Poindexter*, 732 F. Supp. at 154-55.

In his previously filed discovery pleadings, Mr. Mohamud has set out the law demonstrating the importance of the defense perspective in assessing evidence for exculpatory material. CR 27 at 5-6. In brief, as the Supreme Court stated in *Alderman*, the defense is in a unique position to evaluate electronic surveillance and assess its relevance to the facts of a case. *Alderman v. United States*, 394 U.S. 165, 182-84 (1969). As further stated there, “[a]dversary proceedings are a major aspect of our system of justice,” and therefore “[a]s the need for adversary inquiry is increased by the complexity of the issues presented for adjudication, and by the consequent inadequacy of *ex parte* procedures as a means for their accurate resolution, the displacement of well-informed advocacy necessarily becomes less justifiable.” *Id.* at 183-84. The Court’s ability to represent a defendant is limited by the fact that

[a]n apparently innocent phrase, a chance remark, a reference to what appears to be a neutral person or event, the identity of a caller or the individual on the other end of a telephone, or even the manner of speaking or using words may have special significance to one who knows the more intimate facts of an accused’s life.

Alderman, 394 U.S. at 182. The defense perspective is especially critical in cases involving electronic surveillance as “the volume of the material to be examined and the complexity and difficulty of the judgments involved” requires the protections associated with the adversarial process. *Alderman*, 394 U.S. at 182 n.14.

Finally, as the Court has previously been advised, defense counsel for Mr. Mohamud have had security clearances and been dealing appropriately with classified information for many years. Indeed, where defense counsel possess the requisite security clearances, the government may be required to justify the necessity of an *ex parte* filing under CIPA for authorization to delete classified

information from discovery documents. *See United States v. Libby*, 429 F. Supp. 2d 18 (D.D.C. 2006). Here, due process requires broad disclosure under FISA and CIPA.

D. Whether Or Not The Court Orders Disclosure So That Mr. Mohamud Can Participate Meaningfully On His Motion To Suppress, This Court's Review Of The FISA Warrant Or Warrants Is *De Novo*.

This Court should review the FISA applications and orders *de novo*. *United States v. Hammoud*, 381 F.3d 316, 332 (4th Cir. 2004) (noting district court's *de novo* review and conducting its own *de novo* review of FISA materials), *vacated on other grounds*, 543 U.S. 1097 (2005); *United States v. Squillacote*, 221 F.3d 542, 554 (4th Cir. 2000) (same); *see also United States v. Campa*, 529 F.3d 980, 991 (11th Cir. 2008); *United States v. Nicholson*, No. 09-CR-40-BR, 2010 WL 1641167, at *5 (D. Or. April 21, 2010).

Several courts have stated that a reviewing court is to conduct essentially the same review of the FISA application and associated materials that the FISC initially conducted upon receiving an application requesting an order under FISA. *In re Grand Jury Proceedings of Special April 2002 Grand Jury*, 347 F.3d 197, 204-05 (7th Cir. 2003); *Mubayyid*, 521 F. Supp. 2d at 131. As such, the court reviews, first, the adequacy of the FISA materials at issue “*de novo* with no deference accorded to the FISC’s probable cause determinations,” and second, the Executive Branch’s certifications, which are reviewed for clear error. *Rosen*, 447 F. Supp. 2d at 545.

As articulated below in Section E, the limitation on independent assessment of the Attorney General’s certifications in a warrant application (50 U.S.C. §§ 1802; 1822) calls into question the constitutionality of the FISA process. To the extent *In re Grand Jury Proceedings* holds that the

standards for FISC and this Court's review are the same, Mr. Mohamud believes it is incorrect. As a result, this Court should not limit its review to consideration of the clearly erroneous standard.

If the Court does not permit meaningful defense participation in the suppression motion, *de novo* review is even more important. Under such circumstances, *de novo* review is hindered because the reviewing court's consideration of the FISA materials is "unaided by the adversarial process." *Rosen*, 447 F. Supp. 2d at 545 (rejecting the government's contention that the FISC's probable cause determination should be accorded "substantial deference"); *Warsame*, 547 F. Supp. 2d at 990 (same). As a result, the most robust review possible is required.

Review by the criminal court should be more exacting than review by the FISC for yet another reason. Once criminal proceedings have been initiated, and the FISA activity has moved out of the realm of intelligence gathering and is being used to seek a conviction and imprisonment of a United States citizen, additional judicial scrutiny is appropriate. The focus at this stage should be on the rights of the defendant against whom the government is acting, rather than the more general interests in intelligence.

In conducting its review, the Court should also be conscious of the distinction in perspective between judicial and executive officials. As the Supreme Court has stated, "[t]he Fourth Amendment does not contemplate the executive officers of Government as neutral and disinterested magistrates. Their duty and responsibility are to enforce the laws, to investigate, and to prosecute." *United States v. United States District Court (Keith, J.)*, 407 U.S. 297, 316-17 (1972); *see also Coolidge v. New Hampshire*, 403 U.S. 443, 450 (1971) (holding that an Attorney General cannot issue a valid warrant and that "prosecutors and policemen simply cannot be asked to maintain the

requisite neutrality with regard to their own investigations”); *Reynolds*, 345 U.S. at 9-10 (noting that “[j]udicial control over the evidence in a case cannot be abdicated to the caprice of executive officers”).

In *United States v. Leon*, the Supreme Court relied on the “detached and neutral role” of the magistrate in issuing search warrants as a check on the conduct of law enforcement. 468 U.S. 897, 926 (1984). This neutrality explains why, in the context of an ordinary warrant, a magistrate’s probable cause determination is entitled to substantial deference. *Id.* at 914. The role of a FISC judge is slightly, but significantly, different than that of an ordinary judge or magistrate. First, the statute directs deference to the executive certifications. Second, FISA authorizations are the *raison d’être* for a FISC judge, and the applications and orders are surrounded by almost complete secrecy. All of these factors call for exacting review of FISA activity.

In considering review of motions to suppress evidence obtained from a FISA warrant, it is also important to bear in mind that the reasoning of *Leon* can not be transferred to the FISA context. When the purpose of a FISA authorization is gathering foreign intelligence information, and its use in criminal prosecutions is secondary, the systemic costs of suppression are lower than in the regular criminal case. The government may still use the intelligence information it has gathered, the primary, or at least significant, purpose for which it acted. See *United States v. Sarkissian*, 841 F.2d 959, 965 (9th Cir. 1988). Whether or not the Court orders disclosure, its review should be exacting.

E. In The Event The Court Does Not Allow Defense Participation Regarding FISA Searches And Seizures, The Court's Review Should Include Consideration Of Potential Constitutional Violations Stemming From The Statute And Its Application In This Case.

As is apparent in the preceding sections of this memorandum, review of the issues raised by Mr. Mohamud's motion to suppress requires the Court to engage in interpretation and construction of a number of provisions of FISA. To the extent the government disagrees with Mr. Mohamud's interpretations, or the Court is inclined to side with some of the courts that have read the statute more broadly, review in this case will require consideration of the constitutionality of the statute. In this section, Mr. Mohamud articulates a number of reasons why a broad reading of FISA, particularly as amended by the Patriot Act, would violate Fourth, Fifth, and Sixth Amendment rights. As in all cases, the Court's review should proceed under the basic rule of statutory construction that, where a plausible reading of a statute would avoid serious constitutional problems, the Court should follow that construction instead of a construction that raises serious constitutional issues. *See Skilling v. United States*, 130 S.Ct. 2896, 2940 (2010). To the extent the Court does not narrowly read the statute, the procedures it purports to authorize should be found to violate the Constitution.

Although a number of the challenges raised here have been rejected by other courts both before and after 2001, the Court should consider the claims in light of the facts of this case, amendments to the Patriot Act, and the lack of Supreme Court authority upholding such claims. *See, e.g., Belfield, supra; United States v. Nicholson*, 955 F. Supp. 588, 590 (E.D. Va. 1997). Consideration of the constitutionality of the statute in light of the facts of this case is required under *United States v. Posey*, 864 F.2d 1487, 1491 (9th Cir. 1989) (the constitutional challenges to FISA must assert deprivation of the specific defendant's rights).

Before FISA was enacted, and for the first 25 years of its existence, the “primary purpose” for surveillance or searches was required to be intelligence gathering. *United States v. Truong Dinh Hung*, 629 F.2d 908, 912-13 (4th Cir. 1980). The non-criminal purpose standard was essential to the cases upholding FISA’s constitutionality. In the Patriot Act of 2001 and a subsequent decision of the FISC, the primary purpose test was abandoned. The change requires reconsideration of FISA’s constitutionality given the use of FISA for normal criminal purposes for governmental intrusions, which implicate the Fourth, Fifth, and Sixth Amendments.

1. The Standard And Procedures For Admissibility Of FISA-Generated Evidence, As Amended By The Patriot Act And Subsequently Interpreted By The Foreign Intelligence Surveillance Court Of Review – That Foreign Intelligence Gathering May Constitute Merely Some Purpose For The Electronic Surveillance Under FISA – Violates The Fourth Amendment’s Prohibition On Unreasonable Searches And Seizures.

When the government first urged the Supreme Court to recognize an intelligence-gathering exception to the Fourth Amendment, it did so based on the argument “that these surveillances are directed primarily to the collecting and maintaining of intelligence with respect to subversive forces, and are not an attempt to gather evidence for specific criminal prosecutions.” *United States District Court (Keith, J.)*, 407 U.S. at 318-19; *see also United States v. Smith*, 321 F. Supp. 424, 428 (C.D. Cal. 1971) (“[t]he government has emphasized that the purpose of the surveillance involved was not to gather evidence for use in a criminal prosecution but rather to provide intelligence information needed to protect against the illegal attacks of such organizations”) (internal quotation marks omitted). Based on that argument, the Supreme Court opened the door to a foreign intelligence exception.

The “primary purpose” standard was then incorporated into FISA when it was enacted in 1978.⁴ The statute also limited the ability of intelligence agencies to share information with law enforcement agencies. *In re Sealed Case*, 310 F.3d at 724. Thirty years later, that rationale was abandoned based on the concern that the wall between intelligence and law enforcement was undermining national security. *Id.* at 729. The shift in the rationale undermines the arguments that justified the use of the foreign intelligence exception in the first place, calling into question the legitimacy of use of FISA-derived evidence in criminal cases.

a. The Devolution Of The Standard For Issuing FISA Warrants.

(1) The Initial Statutory Language of FISA

When FISA was enacted in 1978, the statute provided that, in order to obtain a surveillance order from a designated FISA judge, the government was required to show probable cause to believe that the prospective surveillance target was a “foreign power” or an “agent of a foreign power.” 50 U.S.C. § 1804(a)(3)(A). It was also required to certify, among other things, that “the purpose” of the surveillance was to obtain “foreign intelligence information.” § 1804(a)(6)(B) (former).

(2) Initial Court Interpretation: The “Primary Purpose” Standard

Shortly after its enactment, the government began to seek admission of FISA-generated evidence in criminal proceedings, resulting in motions to suppress on constitutional grounds. The courts, in determining whether FISA-generated evidence could be admitted at a criminal trial, refined the statutory standard and uniformly held that such evidence was admissible as long as the government’s “primary purpose” in conducting the electronic surveillance (and, later, searches

⁴ The statute used the word “purpose.” *infra* at 34.

performed pursuant to FISA) was the acquisition of foreign intelligence information (as opposed to information to build a criminal investigation of the target of the eavesdropping or search). *See, e.g., United States v. Duggan*, 743 F.2d 59, 77 (2d Cir. 1984).

(3) The Patriot Act Amendments: The “Significant Purpose” Standard

In October 2001, following the events of September 11, 2001, and as part of the Patriot Act, Pub. L. No. 107-56, 115 Stat. 272, § 218, Congress, without any debate, amended 50 U.S.C. §§ 1804(a)(6)(B) and 1823(a)(6)(B) of FISA to permit FISA warrants when the government’s foreign intelligence-gathering purpose was “significant” (as opposed to the pre-existing “primary” purpose standard).

The Patriot Act amendments, by reducing the standard to a “significant” purpose, dramatically expanded the class of investigations in which FISA is available to the government. The amendments authorized the government, for the first time, to obtain surveillance orders under FISA’s relatively undemanding standards even when its primary purpose is to gather evidence of criminal activity. The consequence is that, in a wide range of criminal investigations, the government can now evade the Fourth Amendment merely by asserting a desire to gather foreign intelligence information from the person it in fact intends to prosecute.

(4) The FISC’s November 2002 Opinion: “Measurable Purpose”

In November 2002, the Foreign Intelligence Surveillance Court met for the first time in a proceeding to hear an appeal by the government. The FISC had rejected procedures proposed by the government subsequent to the Patriot Act amendments. In the course of reversing the FISC’s rejection of certain minimization protocols, the FISC further diluted the standard the government

must meet for approval of FISA warrant applications.⁵ After reversing the FISC and acknowledging that “the constitutional question presented in this case . . . has no definitive jurisprudential answer[.]” 310 F.3d at 746, the FISCRC nevertheless explicitly upheld the constitutionality of FISA as amended by the Patriot Act. *In re Sealed Case*, 310 F.3d at 746.

In the course of its analysis, the FISCRC addressed the question whether FISA orders are warrants within the meaning of the Fourth Amendment. The FISCRC acknowledged the significant differences between FISA’s procedural requirements and those of Title III. The FISCRC concluded, “to the extent the two statutes diverge in constitutionally relevant areas . . . a FISA order may not be a ‘warrant’ contemplated by the Fourth Amendment.” *In re Sealed Case*, 310 F.3d at 741. The FISCRC declined to decide the issue, however, and instead proceeded directly to the question whether FISA electronic surveillance and searches are reasonable, concluding:

[W]e think the procedures and government showings required under FISA, if they do not meet the minimum Fourth Amendment warrant standards, certainly come close. We, therefore[] believe firmly . . . that FISA as amended is constitutional because the surveillances it authorizes are reasonable.

⁵ The precise issue before the FISCRC was the propriety of the 2002 Procedures, and not FISA’s constitutionality. The FISCRC could have easily decided that question – an internal Department of Justice administrative protocol matter – without addressing FISA’s post-PATRIOT Act constitutionality. However, the FISCRC chose to confront the constitutional issue in a portion of its opinion that constitutes *dicta*. That section’s status as *dicta* is reinforced by the fact that neither the target of the particular surveillance orders that gave rise to the FISCRC’s ruling, nor anyone arguing that FISA was unconstitutional, was allowed to participate as a party (although the FISCRC did accept an *amicus* brief from the American Civil Liberties Union and civil rights groups, and another *amicus* brief from the National Association of Criminal Defense Lawyers). Oral argument on appeal was closed to the public and conducted *ex parte*.

Id. at 746.⁶

In ruling, the FISCER construed the Patriot Act amendments to add “measurable” to the standard:

The addition of the word “significant” to section 1804(a)(7)(B) imposed a requirement that the government have a measurable foreign intelligence purpose, other than just criminal prosecution of even foreign intelligence crimes.

Id. at 735 (emphasis); *see also id.* (“significant purpose” test “excludes from the purpose of gaining foreign intelligence information a sole objective of criminal prosecution”). The FISCER recognized that its view “may not make much practical difference[]” from the government’s position that even a wholly criminal purpose was permissible, since “[s]o long as the government entertains a realistic option of dealing with the agent other than through criminal prosecution, it satisfies the significant purpose test.” *Id.*

The FISCER’s construction of the “significant purpose” standard – regardless of whether it is phrased as “measurable foreign intelligence purpose,” or excluding “a sole objective of criminal prosecution,” or a “realistic option” of treatment other than criminal prosecution – effectively eliminates the standard altogether, and leaves the government free to employ FISA surveillance for criminal investigatory purposes at will. It is those standards – both the “significant” purpose standard in the Patriot Act and/or the further weakened test articulated by the FISCER – that are the subject of the challenge that they do not measure up to the requirements of the Fourth Amendment.

⁶ Because the FISCER ruled in favor of the government, there was no party to appeal the decision to the Supreme Court. Although *amici* moved to intervene directly in the Supreme Court for the purpose of filing a petition for certiorari, the Supreme Court denied the motion without opinion. *See American Civil Liberties Union v. United States*, 538 U.S. 920 (2003).

They also underscore the deficient protections of Fifth and Sixth Amendment interests inherent in the statute.

b. The “Primary Purpose” Standard Was Essential To FISA’s Constitutionality.

The diminution of the standard from “primary” to “significant,” or even to “measurable,” or not “solely” for criminal investigatory purposes, is constitutionally unsupportable. The courts had previously developed the “primary purpose” standard in order to preserve FISA’s constitutionality, and not because FISA itself required as much. Nor was the “primary purpose” standard promulgated to create any rights for defendants that were not already provided by the Fourth Amendment.

(1) The “Primary Purpose” Standard Predated FISA.

The “primary purpose” standard existed as a constitutional necessity before FISA was enacted. In *Keith*, the Supreme Court rejected the government’s assertion that it could conduct warrantless domestic electronic surveillance pursuant to a purported “national security” exception to the Fourth Amendment. The Court expressly left open the question of warrantless *foreign* intelligence surveillance. 407 U.S. at 321-22; *see also Smith*, 321 F. Supp. at 428-29. After *Keith*, several Circuit courts recognized a *foreign* intelligence exception to ordinary Fourth Amendment requirements.

Critically, these courts emphasized that the exception was limited to intelligence surveillance, and could not be relied on as a justification for disregarding ordinary Fourth Amendment requirements in criminal investigations. Thus, in *Truong Dinh Hung*, the Fourth Circuit recognized a foreign intelligence exception to ordinary Fourth Amendment requirements but strictly limited the

exception to cases in which “the surveillance is conducted primarily for foreign intelligence reasons.” 629 F.2d at 915.

The exception applies only to foreign powers, their agents, and their collaborators. Moreover, even these actors receive the protection of the warrant requirement if the government is primarily attempting to put together a criminal prosecution.

Id. at 916. While *Truong* was not decided until 1980, it involved surveillance that took place before FISA’s enactment in 1978. *Id.* at 915 n.4.

Other Circuits acknowledged a foreign intelligence exception before FISA’s enactment, adopting similar reasoning. *See, e.g., United States v. Butenko*, 494 F.2d 593, 606 (3d Cir. 1974) (“Since the primary purpose of these searches is to secure foreign intelligence information, a judge, when reviewing a particular search must, above all, be assured that this was in fact its primary purpose and that the accumulation of evidence of criminal activity was incidental.”); *United States v. Brown*, 484 F.2d 418, 427 (5th Cir. 1973) (“The serious step of recognizing the legality of a warrantless wiretap can be justified only when, as in the case before us, the foreign and sensitive nature of the government surveillance is crystal clear.”) (Goldberg, J., concurring). Importantly, each of these cases involved surveillance conducted before FISA was enacted – that is, before there was any statutory basis for a primary purpose restriction. Thus, the basis for the restriction was found not in the statute but in the Constitution. The Fourth Circuit made this abundantly clear:

[T]he executive can proceed without a warrant only if it is attempting primarily to obtain foreign intelligence from foreign powers or their assistants. We think that the unique role of the executive in foreign affairs and the separation of powers will not permit this court to allow the executive less on the facts of this case, but *we also are convinced that the Fourth Amendment will not permit us to grant the executive branch more.*

Truong, 629 F.2d at 916 (emphasis added).

(2) The Courts Adopted the Pre-Existing “Primary Purpose” Standard for FISA In Order to Preserve Its Constitutionality.

FISA as originally enacted did not expressly include a “primary purpose” requirement. Most courts that considered FISA’s constitutionality, however, generally interpreted the “purpose” requirement as a “primary purpose” requirement in order to keep FISA consistent with the Fourth Circuit’s view that the Constitution does not permit the government to rely on the foreign intelligence exception where its primary purpose is to gather evidence of criminal activity. *See, e.g., United States v. Johnson*, 952 F.2d 565, 572 (1st Cir. 1991) (stating that “the investigation of criminal activity cannot be the primary purpose of the surveillance,” and that FISA may “not be used as an end-run around the Fourth Amendment’s prohibition of warrantless searches”); *United States v. Pelton*, 835 F.2d 1067, 1074-76 (4th Cir. 1987) (interpreting “purpose” to mean “primary purpose”); *United States v. Badia*, 827 F.2d 1458, 1464 (11th Cir. 1987); *United States v. Duggan*, *supra*.

The Ninth Circuit recognized a foreign intelligence exception to the Fourth Amendment’s ordinary requirements in *United States v. Cavanagh*, 807 F.2d 787, 790 (9th Cir. 1987). Later, the Ninth Circuit expressly declined to reach the question whether the Constitution permits the government to rely on the exception where its primary purpose is to gather evidence of criminal activity. *Sarkissian*, 841 F.2d at 964. In *Sarkissian*, the defendant challenged a district court’s refusal to suppress evidence obtained under FISA, arguing that the government’s purpose in effecting the surveillance was criminal investigation and that, consequently, the surveillance should have been effected under Title III rather than FISA. The Court rejected the defendant’s argument, holding that

“[r]egardless of whether the test is one of purpose or primary purpose, . . . it is met in this case.” *Id.* at 964.

Assuming that the government sought the warrant or warrants at issue in this case based on the statutory standard, or that standard as modified by the FISCER, use of their fruits against Mr. Mohamud would violate his Fourth Amendment rights. As articulated above, while it may be permissible to issue warrants on the lower standard for intelligence purposes, the fruits of those warrants may not be used in a criminal case against the target of the warrants.

- (3) If the Warrants In This Case Were Issued Using The FISA Or FISCER Standard And Generated Information Supporting Investigation Of Criminal Activity, Any Extensions Violated The Fourth Amendment.

The defect in the FISA process is most apparent with respect to extensions of FISA warrants. Whatever justification may exist to allow use in a criminal case of information derived from FISA warrants on its lower standard would evaporate if the government obtained information about criminal activity and then sought an extension. The situation would then be analogous to seizing containers found in plain view and searching without a warrant. *United States v. Jacobson*, 466 U.S. 109, 114 (1984) (even lawfully seized containers cannot be opened without a warrant); *Texas v. Brown*, 460 U.S. 730, 741-42 (1983) (concurrence) (can seize movable closed container in plain view if there is probable cause to believe it contains contraband but must obtain warrant before opening it). If the government learns of criminal activity through a FISA warrant and then desires to continue surveillance knowing it will initiate a prosecution, the normal requirements of the Fourth Amendment should be followed.

- (4) The “Significant Purpose” And/Or The FISC’s More Diluted Standard Fail To Meet Fourth Amendment Requirements For Criminal Investigations.

Regardless of whether the Patriot Act’s “significant” purpose standard, or the weaker construction posited by the FISC is utilized, under a broad reading of the statute, their use to authorize FISA warrants violates the Fourth Amendment in several respects.

- (i) FISA Authorizes Warrants In The Absence Of The Judicial Review Required Under The Fourth Amendment.

One of the core concepts of the Fourth Amendment is that a neutral and detached magistrate must stand between the government and the privacy of its citizens. *Coolidge*, 403 U.S. at 450 (1971). In order to conduct a search or surveillance in an ordinary criminal investigation, the government must obtain the prior authorization of a neutral, disinterested magistrate who has the authority to determine whether the requirements of Rule 41 or Title III have been satisfied. *See* FED. R. CRIM. P. 41 (governing physical searches in criminal investigations); 18 U.S.C. §§ 2518(1)(b), (2) & (3) (governing electronic surveillance in criminal investigations); *see Johnson v. United States*, 333 U.S. 10, 13-14 (1948).

FISA reduces the authority of judges reviewing warrants issued under its provisions. The FISC does not have full authority to determine whether, in any particular investigation, the FBI has satisfied the requirements of FISA. The government satisfies most of FISA’s requirements simply by certifying that the requirements are met. *See* 50 U.S.C. § 1804(a)(6); 1823(a)(6) (enumerating necessary certifications).

While certain (but not all) of these certifications must be accompanied by “a statement of the basis for the certification,” 50 U.S.C. § 1804(a)(6)(E), the statute makes clear that the FISA court

is not to fully scrutinize such statements, but rather is to defer to the government's certification unless it is "clearly erroneous on the basis of the statement made under § 1804(a)(6)(E)." 18 U.S.C. § 1805(a)(4). As the FISC has acknowledged, "this standard of review is not, of course, comparable to a probable cause finding by the judge." *In re Sealed Case*, 310 F.3d at 739 (quoting H. R. REP. NO. 95-1283, at 80 (1978)); *see also Duggan*, 743 F.2d at 77, superseded by statute, PATRIOT ACT, Pub. L. No. 107-56, 115 Stat. 271 (2001), *as recognized by United States v. Abu-Jihaad*, 630 F.3d 102, 130 (2d Cir. 2010). Courts that have approved the judiciary's deference to executive certification fail to recognize the manner in which FISA limits the authority of the FISC. For example, in *United States v. Jayyousi*, No. 04-60001, 2007 WL 851278, at *5 (S.D. Fla. Mar. 15, 2007), the court stated, "the FISC retains all of the 'inherent powers that any court has when considering a warrant . . .'" *See also In re Kevork*, 634 F. Supp. 1002, 1014 (C.D. Cal. 1985). This is simply inconsistent with the limitation on review in §§ 1804(a)(6)(E); 1823(a)(6)(E).

Prior to the Patriot Act amendment, it may have been reasonable to limit judicial review of warrant applications. Once, however, the use of warrants was permitted even when the "primary purpose" was no longer intelligence gathering, the rationale for limiting the judiciary's role can no longer stand under the Fourth Amendment. The protections of the people's right against government intrusions for criminal investigatory purposes required by the Fourth Amendment must be present if the government is to use evidence in a criminal prosecution. "A search prosecuted in violation of the Constitution is not made lawful by what it brings to light; and the doctrine has never been recognized by this court, nor can it be tolerated under our constitutional system, that evidences of crime discovered by a federal officer in making a search without lawful warrant may be used against

the victim of the unlawful search where a timely challenge has been interposed.” *Byars v. United States*, 273 U.S. 28, 29-30 (1927). Since surveillance and searches conducted pursuant to FISA here were likely conducted without meaningful prior judicial review, they were unreasonable under the Fourth Amendment.

(ii) FISA Orders Do Not Qualify As Warrants Under the Fourth Amendment.

FISC surveillance orders are not warrants within the meaning of the Fourth Amendment. *See In re Sealed Case*, 310 F.3d at 741 (acknowledging that FISA orders “may not be . . . ‘warrant[s]’ contemplated by the Fourth Amendment”). The Supreme Court has held that a warrant must be issued by a neutral, detached magistrate; must be based on a demonstration of probable cause; must relate a particular offense; and must particularly describe the things to be seized as well as the place to be searched. *Dalia v. United States*, 441 U.S. 238, 255 (1979). FISC orders do not satisfy these requirements. On the contrary, FISA empowers the government to conduct the most intrusive kinds of surveillance with lesser judicial review than required by the Constitution, without showing criminal probable cause, and without meeting particularity requirements. Because FISC orders are not warrants, searches conducted under FISA are presumptively unreasonable. *See, e.g., Payton v. New York*, 445 U.S. 573, 586 (1980); *Chimel v. California*, 395 U.S. 752, 762-63 (1969). The surveillance at issue in this case cannot overcome that presumption. *But see In re Sealed Case*, 310 F.3d at 746.

(iii) FISA Warrants Do Not Satisfy Traditional Probable Cause Standards.

The Fourth Amendment ordinarily prohibits the government from conducting intrusive surveillance without first demonstrating criminal probable cause – probable cause to believe that “the evidence sought will aid in a particular apprehension or conviction for a particular offense.” *Dalia*, 441 U.S. at 255. FISA, on the other hand, appears to authorize the government to conduct intrusive surveillance if it can show what is known as “foreign intelligence probable cause” – probable cause to believe that the surveillance target is a foreign power or agent of a foreign power. *See* 50 U.S.C. § 1805(a)(2)(A).

The government has taken the position that foreign intelligence probable cause bears only a passing resemblance to criminal probable cause. In response to a Freedom of Information Act request filed by the American Civil Liberties Union and others in August 2002, the FBI released, among other things, a document from the FBI’s National Security Law Unit entitled, “What do I have to do to get a FISA?”⁷ At page 2 to 3 of this document, the FBI stated:

[P]robable cause in the FISA context is similar to, but not the same as, probable cause in criminal cases. Where a U.S. person is believed to be an agent of a foreign power, there must be probable cause to believe that he is engaged in certain activities, for or on behalf of a foreign power, which activities involve or may involve a violation of U.S. criminal law. The phrase “involve or may involve” indicates that the showing of [nexus to] criminality does not apply to FISA applications in the same way it does to ordinary criminal cases. As a result, there is no showing or finding that a crime has been or is being committed, as in the case of a search or seizure for law enforcement purposes. The activity identified by the government in the FISA context may not yet involve criminality, but if a reasonable person would believe that such activity is likely to lead to illegal activities, that would suffice. In addition, and with respect to the nexus to criminality required by the definitions of “agent of a

⁷ This document is available at http://www.aclu.org/patriot_foia/FOIA/Sept2002Doc.pdf.

foreign power,” the government need not show probable cause as to each and every element of the crime involved or about to be involved.

Thus, if foreign-intelligence probable cause is not “probable cause” within the ordinary meaning of the Fourth Amendment, the surveillance at issue in this case was likely not premised on criminal probable cause and, accordingly, was unreasonable within the meaning of the Fourth Amendment. As argued above, Mr. Mohamud believes that the government’s interpretation of FISA is incorrect and that, as a United States person, probable cause of criminal activity is required. If this Court does not accept that position, the statute is unconstitutional. *See Skilling, supra*.

(iv) FISA Warrants Do Not Satisfy the Fourth Amendment’s Particularity Requirement.

The electronic surveillance and searches in this case may have lasted over one year, during which the government intercepted thousands of telephone calls, text messages, and e-mails. Although no indication has been provided to date, FISA physical searches may also have intruded into Mr. Mohamud’s home. Because the duration and scope of these intrusions was not strictly limited, the surveillance violated the Fourth Amendment’s particularity requirement.

The Fourth Amendment ordinarily prohibits the government from conducting intrusive surveillance unless it first obtains a warrant describing with particularity the things to be seized as well as the place to be searched. *Berger v. New York*, 388 U.S. 41, 58 (1967) (noting that Fourth Amendment particularity requirement was intended to prevent the government’s reliance on “general warrants” that allow “the seizure of one thing under a warrant describing another”). In *Berger*, the Supreme Court stated that the importance of the particularity requirement “is especially great in the case of eavesdropping.” *Berger*, 388 U.S. at 56. The Court explained: “[B]y its very nature

eavesdropping involves an intrusion on privacy that is broad in scope.” *Id.* “[T]he indiscriminate use of such devices in law enforcement raises grave constitutional questions under the Fourth and Fifth Amendments, and imposes a heavier responsibility on this Court in its supervision of the fairness of procedures.” *Id.*

With respect to eavesdropping devices and wiretaps, the particularity requirement demands not simply that the government describe in detail the communications it intends to intercept, but also that the duration of the intercept be strictly limited. *See Berger*, 388 U.S. at 58-60.⁸ Title III, which Congress enacted shortly after *Berger* was decided, limits the term of surveillance orders to 30 days. 18 U.S.C. § 2518(5). FISA, by contrast, authorizes surveillance terms of up to 90 or 120 days or even one year. 50 U.S.C. § 1805(d)(1); 1824(d)(1). In addition, the Ninth Circuit has confirmed that, at least in the context of criminal investigations, the 30-day limitation is constitutionally required. In *United States v. Koyomejian*, 970 F.2d 536 (9th Cir. 1991) (en banc), the court confronted the legality of silent video surveillance in a domestic criminal investigation. The court held that neither Title III nor FISA speaks to such surveillance but that warrants authorizing silent video surveillance must nonetheless be limited to terms of no more than 30 days. *Id.* at 542.

⁸ The Ninth Circuit’s decision in *Cavanagh*, 807 F.2d at 791, is not to the contrary. The court in *Cavanaugh* considered only the contention that FISA violates the particularity clause by allowing a general description of the information sought; it did not consider, and apparently was not asked to consider, whether the *duration* of FISA surveillance orders renders FISA unconstitutional. Second, *Cavanagh* addressed the particularity issue in the context of a statute whose ambit was limited to foreign intelligence investigations. The question whether FISA meets the particularity requirement in the context of *criminal* investigations was not addressed in *Cavanagh*.

To the extent FISA is read to permit issuance of a warrant – or an extension – without the type of particularity required under Title III, it would violate the Constitution/ *But see Mubayyid*, 521 F. Supp. 2d at 138.

(v) The Fourth Amendment’s “Special Needs” Exception Does Not Apply To FISA.

FISA and its purposes do not justify departure from the Fourth Amendment based on the “special needs” exception. The Supreme Court’s consistent answer to invocation of that exception has been that “[a] search unsupported by probable cause can be constitutional . . . when special needs, beyond the normal need for law enforcement, make the warrant and probable-cause requirement impracticable.” *Vernonia Sch. Dist. 47J v. Acton*, 515 U.S. 646, 653 (1995) (internal quotation marks omitted) (quoting *Griffin v. Wisconsin*, 483 U.S. 868, 873 (1907)).

The Supreme Court reaffirmed this well-settled rule in *Ferguson v. City of Charleston*, 532 U.S. 67 (2001). *Ferguson* involved a public hospital’s policy of testing pregnant patients for drug use and employing the threat of criminal prosecution as a means of coercing patients into substance-abuse treatment. The Court invalidated the policy. “In other special needs cases,” the Court wrote, “we . . . tolerated suspension of the Fourth Amendment’s warrant or probable cause requirement in part because there was no law enforcement purpose behind the searches in those cases, and there was little, if any, entanglement with law enforcement.” *Ferguson*, 532 U.S. at 79 n.15; *see also id.* at 88-9 (Kennedy, J., concurring). In *Ferguson*, however, “the central and indispensable feature of the policy from its inception was the use of law enforcement” *Ferguson*, 532 U.S. at 80. The Court has cautioned that, notwithstanding the seriousness of law enforcement interest with respect to the particular crimes at issue, “the gravity of the threat alone cannot be dispositive of questions

concerning what means law enforcement officers may employ to pursue a given purpose.” *City of Indianapolis v. Edmond*, 531 U.S. 32, 42 (2000). When the government’s “primary purpose [is] to detect evidence of ordinary criminal wrongdoing,” the Fourth Amendment forecloses the government from conducting searches except based on criminal probable cause. *Edmond*. 531 U.S. at 38.

Nor is *In re Sealed Case* availing to the government. The FISCER reasoned that, although the special needs cases apply only where the government’s primary purpose is not law enforcement, the relevant question is not the immediate purpose of a FISA search but rather FISA’s “programmatic purpose.” 310 F.3d at 745. In fact, the Supreme Court has emphatically rejected that argument. In *Ferguson*, for example, the government argued that the relevant question was the government’s “ultimate purpose,” and that the ultimate purpose of the hospital’s policy was not law enforcement but public health. 532 U.S. at 81. The Court found the law enforcement purpose to be determinative:

the threat of law enforcement may ultimately have been intended as a means to an end, but the direct and primary purpose . . . was to ensure the use of those means. In our opinion, the distinction is critical. Because law enforcement involvement always serves some broader social purpose or objective, under respondents’ view, virtually any nonconsensual suspicionless search could be immunized under the special needs doctrine by defining the search solely in terms of its ultimate, rather than immediate, purpose.

Ferguson, 532 U.S. at 83-84. Similarly, the government’s important interest in criminal prosecution of purported terrorists does not exempt the government from the Fourth Amendment if a substantial purpose is criminal prosecution.

2. The *Ex Parte, In Camera* FISA Process Violates Due Process, A Defendant's Rights To Be Present At All Critical Stages Of The Criminal Process, And His Right To The Effective Assistance Of Counsel.

FISA authorizes the unprecedented exclusion of the accused from critical stages of the prosecution: review of the motion to suppress evidence. The post-indictment procedure, in a criminal prosecution, is conducted *ex parte* and *in camera* and without the defendant ever having the right to even see the warrants or affidavits he is challenging. To permit Mr. Mohamud's motion to proceed in this manner would violate his Fifth and Sixth Amendment rights.

Fundamental to due process is the right to notice and an opportunity to be heard. *See LaChance v. Erickson*, 522 U.S. 262 (1998). The interest at stake is the most fundamental liberty – freedom from incarceration. *Turner v. Rogers*, No. 10-10, 2011 WL 2437010, at *10 (U.S. June 20, 2011) (“Freedom ‘from bodily restraint’ lies ‘at the core of the liberty protected by the Due Process Clause.’”) (quoting *Foucha v. Louisiana*, 504 U.S. 71, 80 (1992)). Equally fundamental is a defendant's right to be present at, and participate in, all critical stages of a criminal prosecution and to be meaningfully assisted by counsel. *See Montejo v. Louisiana*, 129 S. Ct. 2079, 2085 (2009); *Tennessee v. Lane*, 541 U.S. 509, 523 (2004).

To be sure, the Constitution recognizes some limits on a defendant's participation in the criminal process. The government may secure an indictment without his participation. *United States v. Salsedo*, 607 F.2d 318, 319 (9th Cir. 1979). In limited circumstances, the court may review potential evidence *ex parte* to determine whether it is material to the defense. *United States v. Mejia*, 448 F.3d 436, 543-54 (D.C. Cir. 2006). If so, it must be disclosed or the government loses the

opportunity to use it. *Skinner v. Switzer*, 131 S. Ct. 1289, 1300 (2011) (citing *Brady*, 373 U.S. at 87).

The FISA limitations on a defendant's participation are different in kind, allowing the court to determine complex constitutional questions in a non-adversarial setting and in secret. The Constitution forbids such a process. *But see Mubayyid*, 521 F. Supp. 2d at 136. Even there, however, the court noted that "[i]t is of course true that the legality of the surveillance and search would be better tested through the adversarial process; an *ex parte* review is not a perfect substitute for that process". 521 F. Supp. 2d at 130. Although the Supreme Court has not addressed the constitutionality of the FISA process, its holdings in analogous situations make clear that FISA cannot stand.

As early as *Hopt v. Utah*, 110 U.S. 574 (1884), the Court held that a criminal defendant had a right to be present at all critical stages of the criminal proceedings:

[T]hat is at every stage of the trial when his substantial rights may be affected by the proceedings against him. If he be deprived of his life or liberty without being so present, such deprivation would be without due process of law required by the constitution.

Hopt, 110 U.S. at 579. In a more comprehensive review of *ex parte* proceedings in criminal cases, the Court in *In re Oliver*, 333 U.S. 257 (1948), rejected a "secret" contempt proceeding. While acknowledging the fact that Grand Jury proceedings are secret, the Court held: "But those reasons have never been thought to justify secrecy in the trial of an accused charged with violation of the law for which he may be fined or sent to jail." *Id.* at 264. The Court concluded by holding that secret proceedings were incompatible with the rights to due process and public trial:

In view of this nation's historic distrust of secret proceedings, their inherent dangers to freedom, and the universal requirement of our federal and state governments that criminal trials be public, the [Constitution's] guarantee that no one shall be deprived of his liberty without due process of law means at least that an accused cannot be thus sentenced to prison.

Id. at 273.

The unconstitutionality of the type of process authorized by FISA is also supported by *United States v. Abuhamra*, 389 F.3d 309 (2d Cir. 2004). There, in the context of a bail application, the government submitted – and the District Court considered – evidence *ex parte* and *in camera*. The Court rejected one-sided secret proceedings:

Particularly where liberty is at stake, due process demands that the individual and the government each be afforded the opportunity not only to advance their respective positions but to correct or contradict arguments or evidence offered by the other.

Id. at 322. *Abuhamra* also noted that such a procedure not only violated the defendant's due process rights but also the right of public access to criminal trials. *Id.* at 316 n.3, 323; *see also Alderman*, 394 U.S. at 182-84. FISA's *ex parte*, *in camera* process, whatever its legality in the context of foreign surveillance, cannot constitutionally displace the defendant's rights under the Fifth and Sixth Amendments. *See United States v. Coplon*, 185 F.2d 629, 638 (2d Cir. 1950) (finding the refusal to allow the defense to see records the judge reviewed *in camera* to determine if the "taps" led to evidence introduced at trial violated the defendants' constitutional right). "Few weapons in the arsenal of freedom are more useful than the power to compel a government to disclose the evidence on which it seeks to forfeit the liberty of its citizens." *Coplon*, 185 F.2d at 638.

One of the first cases to consider these arguments under FISA was *Belfield*. There, the court rejected similar Fifth and Sixth Amendment claims. 692 F.2d at 148. The court's reasoning was,

however, anchored in the fact that “FISA is concerned with foreign intelligence surveillance.” *Id.* Courts that rejected similar claims after the Patriot Act amendments have failed to recognize the change in the statutory criteria. *See, e.g., United States v. Kashmiri*, No. 09 CR 830-4, 2010 WL 4705159 (N.D. Ill. 2010). Once Congress expanded the purposes of and standards for surveillance, it shifted the constitutional calculus. As stated in *Boumediene v. Bush*, 553 U.S. 723, 797 (2008), “security subsists, too, in fidelity to freedom’s first principles.” Those principles support the conclusion that FISA no longer passes constitutional muster if it shuts criminal defendants out of the process.

3. The FISA “Suppression” Process Unconstitutionally Interferes With The Article III Judicial Power.

Chief Justice John Marshall in *Cohens v. Virginia*, noted that the judicial power of the federal courts “extends to all cases arising under the constitution or a law of the United States, whoever may be the parties.” 19 U.S. (6 Wheat.) 264, 392 (1821). FISA may trigger this judicial power, but it cannot constitutionally expand or restrict the scope of Article III. It does both.

In considering the constitutionality of FISA’s limit on judicial power, “[t]he controlling question is whether the function to be exercised by the court is a judicial function.” *Fed. Radio Comm’n v. Nelson Bros., Co.*, 289 U.S. 266, 277 (1933). An Article III court determining a Fourth Amendment suppression motion on a federal indictment surely performs a “judicial function.”

The first defect in FISA under Article III is that it permits the courts to act when there is case or controversy. *Camreta v. Green*, 131 S. Ct. 2020, 2028 (2011) (“Article III of the Constitution grants this Court authority to adjudicate legal disputes only in the context of “Cases” and “Controversies.”). The role of the courts is to resolve disputes between or among parties. *Principal*

Life Ins. Co. v. Robinson, 394 F.3d 665, 671 (9th Cir. 2005). They may not issue advisory opinions. *Sierra Club v. Morton*, 405 U.S. 727, 732 n.3 (1972). Contrary to these principles, FISA permits the courts to act in a one-sided manner, treating the question of suppression as if only one party had an interest sufficient to warrant judicial action.

The second defect in FISA is that it limits the Judiciary's Article III powers by requiring the courts to defer to executive assertions in a criminal case. 50 U.S.C. §§ 1805(a)(4), 1824(a)(4). The fact that FISA gives the Attorney General undue control of the warrant and suppression motion processes and limits FISA review infringes on the judicial responsibility to say what the law is, as it "is a responsibility of this Court as ultimate interpreter of the Constitution." *Baker v. Carr*, 396 U.S. 186, at 211 (1962). *See Kendall v. United States*, 37 U.S. 524, at 526 (1838) (discerning judicial authority and separation of powers).

The third defect is that FISA, as implemented *ex parte* and *in camera*, violates the separation of powers inherent in the first three Articles of the Constitution. While the Executive Branch must assure that the laws are faithfully executed, the Judiciary ultimately must decide whether the executive action complies with legislative standards. By conferring deference to the Executive while excluding the citizen, the separation of powers is breached, with the citizen ineffectively protected from executive overreaching.

The judicial power to conduct a Fourth Amendment suppression hearing flows directly from Article III of the Constitution. It does not flow from, nor can it be limited by, a purported congressional delegation to the Attorney General, who in turn tells this Court how to exercise its judicial powers and discretion in a bona fide constitutional "case and controversy."

Conclusion

For the reasons stated above, we respectfully submit that grounds may exist for an order suppressing the evidence obtained pursuant to FISA because the government violated FISA and FISA is unconstitutional as applied in this case. Accordingly, the defense respectfully requests production of the application materials that were submitted to the FISC, the warrant or warrants that were used to intercept the communications or otherwise obtain evidence against Mr. Mohamud, and all material derived from any FISA warrants. The defendant has a right to a meaningful role in determination of the legality of FISA surveillance and searches and the Court should assure a rigorous and fair adversary process.

Respectfully submitted this 22nd day of June, 2011.

/s/ Stephen R. Sady

Stephen R. Sady
Chief Deputy Federal Public Defender

Steven T. Wax
Federal Public Defender

Ruben Iñiguez
Assistant Federal Public Defender